BANGALORE ELECTRICITY SUPPLY COMPANY LIMITED

Tender Enquiry No: BESCOM/2024-25/SE0226 dated 28.11.2024

Section-IV

TECHNICAL SPECIFICATION

Supply, Install, Test, Commission and Integration of Communication Equipment for SCADA operations of SPB with Control Centres equipment and remote devices pertaining to North zone of BMAZ

Issued By

General Manager (DAS)
Corporate office, BESCOM
BESCOM Integrated Control Center-1,
17th cross, 24th Main,
Sector-2, HSR layout
Bangalore-560102

E-mail ID: gmdas@bescom.co.in
Mobile No.:9448279010
Office No.:080-22586356

Table of contents

1. Introduction 3
2. Scope of Work 3
3. Project Support Activities 4
4. Project Responsibilities 4
4.1 Contractor Responsibilities 4
4.2 Employer Responsibilities 5
5. Applicable Standards 6
6. Communication System Specifications 6
6.1 General Requirements 6
6.2 Service Conditions 7
6.3 Electric Surge Protection 8
6.4 Power Supplies and Enclosures 8
7. Technical Specifications 8
7.1 Remote End Equipment 8
7.2 Firewall at control centre 10
7.3 Network Management System 12
7.4 Cyber Security: 17
8. Training 17
9.Testing and Inspection 17
9.1 Factory Inspections and Tests 18
9.2 Shipment 18
9.3 Link Establishment / Commissioning Tests 18
9.4 Availability Test 19
9.5 Integrated System Test 19
10. Warranty and AMC 19
10.1 Warranty details 19
10.2 Annual Maintenance Contract 19
10.3 Service Level Agreement 19

1. Introduction

BESCOM has implemented Distribution Automation System (DAS) for monitoring, supervisory control and operation of 11kV distribution network in Bengaluru city to improve power supply availability to consumers, reduce interruption duration and manage power supply. DAS has facilitated rapid restoration of power supply to consumers who are not connected to a fault and early rectification of fault thus reducing interruption duration and also manage power supply.

To facilitate DAS operations, 3130 SCADA 11kVswitch gears (RMUs: 1590 Nos, LRC / LBS: 1540 Nos.) were installed. The status and analog details of these switch gears are transmitted to DAS Control Centers located in HSR Layout and Rajajinagar through BESCOM's own RF based licensed communication system.

The objective of the project is to develop a Self-sustained independent communication network for RTU`s communication with Distribution Automation system Control Center`s located at HSR Layout and Rajaji Nagar. This will enable BESCOM for continuous monitoring of power system real time parameters of 11KV SCADA switchgear from DAS control centre. Communication infrastructure proposed is pertaining to the new SCADA enabled switchgears (Single Panel Breakers) being added under Upgradation of DAS project.

This Technical Specification concerns the Communication System to be designed, supplied, installed, commissioned and integrated as part of Communication System expansion for DAS operations in Bangalore City by establishing communication to the Single Panel Breakers.

2. Scope of Work

The scope of work includes design, supply, installation, commissioning and integration of all hardware and software that shall establish a properly functioning Communications System providing reliable, secure, and efficient data communications in support of the DAS operations. In this respect, the intent is to create an integrated communications network that, together with the DAS, shall ensure the lowest achievable latencies and highest speed of data throughput given the constraints of the technology and protocols used for the delivery of data.

The Contractor shall design, supply, install, commission and integrate the automated points with DAS Communication Facility Phase-wise. The list of sites to be covered in each Phase will be provided during the design phase of implementation. Brief scope includes the following.

1. BESCOM intend to integrate all field Remote Terminal Unit with DAS system which are installed inside 11kV switchgears (Single Panel Breaker). For that bidder have to establish complete communication network for integration of RTU`s with control centres.
2. Design, Supply, Installation, Testing and Commissioning of communication equipment at Single Panel Breaker (SPB) site, Firewalls and all required accessories or equipment to establish communication at both Control centres.

3. Providing MPLS Line 50Mbps from ISP to Control Centres with redundancy and proper cyber security measures. Bandwidth will be finalised during design phase of the communication system.
4. Providing M2M (13 digit) MPLS VPN SIMs for operation with minimum 1GB per month.
5. Link demonstration of communication system.
6. Operation and Maintenance of system.
7. Communication logs to be made available.
8. System should be monitored centrally from control centres
9. Remote equipment data to be synchronised between the NMS (replication process) in control centres at real time
10. Antenna and cable for remote end communication to be provided and secured outside of SPB Panel. High gain antenna to be provided in Low Signal strength area.
11. Appropriate alternate communication mode to be established wherever SIM based solution is not working, in order to maintain the availability of the RTU for control centre operations.
12. Contractor will be responsible to coordinate and configure internal network to external network of BESCOM for data routing
13. Provision of any other hardware or software to meet the intent of the communication system.

3. Project Support Activities

To meet the basic communication requirements, the Contractor shall perform all necessary project support activities such as:

1. Project management to include Survey, design, planning, scheduling, supervising, and coordinating work, preparing progress reports, and attending meetings, etc. Coordination shall include cooperation with BESCOM employees to fully integrate to the existing network.
2. System Factory testing, Installation, integration and Commissioning activities.
3. Training courses for Employer personnel
4. All required documentation, e.g., functional design documents, test procedures, test reports, user manuals, Training documents etc.
5. After-sales warranty and support services.

4. Project Responsibilities

The Employer and Contractor will take responsibility for various Communication System tasks. Some of the responsibilities are described below. Otherwise, specific responsibilities concerning the Contractor in particular are described elsewhere in these Technical Specifications.

4.1 Contractor Responsibilities

The Contractor shall be responsible for designing, supplying, installing, commissioning and integrating the required communication equipment in good working order and fit for its intended purpose.

1. Detailed Survey and design of the communication network.
2. Providing and configuring remote end device with proper signal strength for DAS operations.
3. Configuration and integration of all field devices to central device.
4. Integration with existing communication network and data routing.
5. Providing NMS software for maintenance and monitoring of the communication network
6. Providing training to BESCOM personnel regarding the communication system.
7. Any defective/Non-Communicating/Burnt equipment to be picked up by the contractor on its own cost. Repairing allowed for minor defects but for major component failure, replacement with new equipment to be done with in Warranty Period.
8. Deploying Engineer during implementation period to ensure the seamless execution and field troubleshoot if any.
9. Its supplier's responsibility to communicate with Network service provider on behalf of BESCOM to ensure seem less communication and troubleshooting if any.
10. All interactions with other agencies and third parties like the basic service provider during the currency of the contract, which may be required for the provisioning of services as per contract.
11. Cooperation of different contractors as they work with the Employer in a combined effort to attain the objectives of the project. Commissioning in particular requires contractors to work in full cooperation for NMS configuration, remote end equipment configuration with SPB RTU.
12. Coordination with South Zone Communication equipment contractor for NMS configuration and data routing.
13. Demonstration of the bandwidth availability to the BESCOM as and when required.
14. The Bandwidth should be on 1:1 from Telecom Provider Gateway for MPLS line connectivity to control centre
15. Telecom Provider should have ISO 27001 certification
16. Configuration of internal network to external network.
17. Maintaining link availability as per SLA requirement

4.2 Employer Responsibilities

Employer responsibilities in support of the Communications System scope of work will include:

1. Provision of control centre, service centre, substation, and RTU location details.
2. Provision of a 230 Vac power source at control centres
3. Ensuring the site availability along with 230V AC and 24 Vdc sources of power.
4. Provision of drawings corresponding to existing network.
5. Review and approval of design drawings, FAT / SAT procedure and Training documents provided by the Contractor.
6. Witnessing during FAT & SAT.
7. Approval of Contractor-provided work plans for installing the communications equipment.
8. Coordination and inspection of the Contractor's field work.

9. Participation in Contractor-provided training courses

5. Applicable Standards

The Employer requires that all work manufactured or furnished under this specification shall comply with the latest applicable IS / IEC standards and its amendments. Exceptions shall be documented and submitted for Employer approval.

Equipment confirming to other internationally accepted standards, which ensure equal or higher quality than the standards mentioned above is also acceptable. In case bidders who wish to offer material confirming to the other standards, salient points of difference between the standards adopted and the specific standards shall be clearly bought out in the relevant schedule.

Equipment shall comply with these following IS / IEC standards and its latest amendments.

1	Impulse voltage test	IEC-61000-4-5(95-03)
2	Insulation resistance test	IS-13779:1999
3	Electrostatic Discharge (ESD)	IEC-61000-4-2 (1995-02)
4	Electromagnetic radiated HF susceptibility	IEC-61000-4-3 (1995-02)
5	Fast transient Burst test	IEC-61000-4-4 (1995-02)
6	Surge Immunity test	IEC61000-4-6

6. Communication System Specifications

The following specifications present the requirements that apply to all communication equipment to be provided by the Contractor except as otherwise noted.

6.1 General Requirements

All communications equipment shall be designed, fabricated, assembled, finished, and documented with workmanship of the highest production quality and shall conform to all applicable quality control standards of the original manufacturer and the Contractor. All components shall be of current production from reliable component manufacturers.

To satisfy these Technical Specifications, manufacturer standard designs shall be used to the fullest extent possible. Relevant type test certificates and results shall be submitted with the bid. The certification shall not be older than five years prior to the Effective Date of Contract.

All materials comprising the communication equipment shall be new and unused and consist of the best industrial grade. Materials promoting the growth of fungus or susceptibility to corrosion and heat degradation shall not be used. In addition, steps shall be taken to provide rodent proof installations.

To facilitate expansion and maintenance, modularity shall be employed in the design of the equipment. All major subassemblies shall carry permanent labels providing a cross-reference to the Contractor's documentation.

All features of the proposed equipment, as described in the Contractor's bid and in the bid's reference materials, shall be fully supported by the equipment actually delivered.

6.1.2 Maintainability

The Employer prefers communication equipment designs that do not require periodic preventive maintenance and inspections. If periodic maintenance is required, it shall be possible to perform all such work in the field without dismounting the equipment and without requiring that the associated medium or high voltage circuit be de-energised.

6.2 Service Conditions

Unless otherwise specified, the communication equipment including any supporting equipment shall be suitable for rated operation under the following service conditions:

1. Operation at elevations of at least 1,000 meters above sea level.
2. Ambient conditions dependent on where the device is installed (indoors or outdoors) as stated in the following sub-clauses.

Suitably accredited test laboratories that are independent of the bidder and equipment manufacturer shall have performed the type tests. Certified copies of the type test certificates and test results shall be included as part of the bidder's proposal.

6.2.1 Indoor Equipment

Though indoor communication equipment installed in control centres may operate in air-conditioned rooms, they shall be capable of operating in rooms (such as Service Centre rooms) that may not be air-conditioned or where the air-conditioning has failed. Conduits and fittings shall be provided for the project's electrical and communication cable system and a complete assembly of conduit, tubing or duct with fittings shall also be provided. Consequently, this equipment shall be suitable for rated operation under the following controlled and uncontrolled service conditions:

1. Ambient air temperatures between 10 and 60 °C.
2. Relative humidity averaging up to 95% (non-condensing).

6.2.2 Outdoor Equipment

All outdoor equipment provided by the Contractor, to be installed in outdoor enclosures shall be suitable for continuous operation in India's tropical monsoon climate, which includes exposure to severe frequently occurring thunderstorms. This equipment shall also be suitable for conditions in which they may be exposed to heavy industrial pollution and high levels of airborne dust.

Equipment shall be suitable for rated operation under service conditions such as:

1. Ambient air temperatures of at least 60 °C.
2. Relative humidity of at least 95% (non-condensing).

6.3 Electric Surge Protection

All external connections for the communication equipment including communication ports, communication lines, and power supply inputs and outputs shall be designed to withstand the fast transient and surge voltage. The communications equipment shall be capable of withstanding the tests without damage, loss of internally stored data and parameters.

6.4 Power Supplies and Enclosures

Power supply and enclosure requirements depend on the location of the communication equipment. This is summarised as follows:

Table 1: Power Supply and Enclosure Requirements

Location of Communication Equipment	**Enclosures**	**Power Supply Source**	
		DC Power	**AC Power**
RTU Site	Provided by Employer	24Vdc Source Provided by Employer	230 Vac Provided by Employer
Control Centre	Provided by Employer	48Vdc Source Provided by Contractor	230 Vac Provided by Employer

Other general requirements are listed as follows:

1. The manufacturer of Remote End device (SD-WAN / Modem) supplied under this contract shall be certified as an ISO 9001 approved facility. A certificate of ISO 9001 certification must be included with the bid documents.
2. Software tools shall be available to allow the remote equipment maintenance and diagnostic data (preferably through SNMP) to be accessed and displayed in graphical form.
3. Hardware and/or software facilities allowing the communication system maintenance and diagnostic data to be accessed via DAS as well as the required field test equipment, shall be included. This feature of the communication system shall also allow the maintenance and diagnostic data to be viewed on a properly authorised and secure basis from workstations.

7. Technical Specifications

7.1 Remote End Equipment

- The Remote end equipment provided by the contractor will be used for communication between RTU installed at SPB and Control Centres. It shall be required to operate satisfactorily and continuously under the following tropical conditions defined above.

- It shall support point to point and point to multipoint communication with both master and slave mode operations. It shall support dual SIM card with active standby capability that can work with different service providers. Equipment mounting shall be such that SIM card tray can be easily accessible without removing it.
- Equipment shall comply with IP55 degree of protection.
- Remote end communication equipment shall also support network changeover on dual SIM operations with following combinations:
    1. Auto-changeover based on Network availability
    2. Auto-changeover based on predefined priority.
    3. Remote Network Changeover capabilities.
- The supplier shall provide terminal software/interface and adequate port for configuration and diagnosis.
- It shall have auto reconnection facility in case of disconnection to server & all disconnection shall be reported to server. It shall support hardware & software WDT (Watchdog Timer). It shall have facility to auto reboot over disconnection with remote server up to certain defined time.
- It shall support following cellular standards: 3G & 4G cellular network GSM/GPRS/EDGE/UMTS/HSPA+/LTE FDD/LTE TDD.
- It shall support following cellular band: LTE FDD 2600/2100/1800/900/800MHz, UMTS/HSPA+: five-band 800/850/900/1900/2100 MHz, GSM/GPRS/EDGE: quad-band 850/900/1800/1900 MHz.
- It shall support all cellular networks available and approved by Telecom Regulatory Authority of India (TRAI). It shall have 2 No. of Ethernet LAN with 10/100 Mbps RJ45 port. It shall support MPLS, MVPN, IPSec and Open VPN Network connectivity for establishing remote connection between Control centre and RTU. It shall be able to create four (04) VPN tunnels simultaneously with Four (04) different SCADA master servers.
- Remote end equipment shall be powered up with 24V DC +/- 5% and support both Dynamic IP SIM and Static IP SIM and configurable through Local as well as remote server via Web UI or other configuration software. It shall support NAT table routing and TCP, UDP, ICMP, SNMP, NAT, DMZ protocols.
- It shall be designed and constructed in such a way to avoid introducing any danger in use and under normal conditions so as to ensure specially
    1. Personnel safety against electric shock.
    2. Personnel safety against effects of excessive temperature.
    3. Protection against spread of fire.
    4. Protection against penetration of solid objects, dust and water
- It shall be capable to withstand surges and voltage spikes by providing necessary isolation and / or suppression system built in the system. External surge protection device also to be provided.
- Antenna and cable for remote end communication to be provided and secured outside of SPB Panel. High gain antenna to be provided in Low Signal strength area. Antenna mounting arrangement at remote site will be finalized during design stage. Necessary material required is included in the scope of work under remote end equipment and accessories.

- As per TRAI guidelines, 13 digit SIM cards to be used for M2M operation. It is mandatory to support all functionality with 13digit SIM cards and 10 digit SIM cards without any firmware or setting modification. It shall have facility to send SMS to configured mobile (min 2 nos) for selected event.
- All other communications should be blocked other than data exchange from remote to Control centre.
- Equipment should have Mandatory Testing and Certification of Telecommunication Equipment (MTCTE) issued by Ministry of Telecommunication
- For determining health of the device an LED shall be provided which will depict the current functioning status (power on / transmitting data).

7.1.1 Diagnostic Provisions

BESCOM shall be able to remotely monitor diagnostic capabilities from control centre. As a minimum requirement the following remote diagnostic points to be made available at control centre.

1. Signal Strength Level
2. Data connection state
3. Device uptime
4. LAN port Status
5. IP Address

7.1.2 Protocols

DNP3.0 / IP protocol is used for SCADA communication from RTU to Control centre.

7.2 Firewall at control centre

The firewall shall provide protection from possible security threats occurring via the RTU WAN. The design and configuration must adhere to Employers latest cyber security and IT/OT policies.

The Contractor shall provide security firewalls to prevent access to the System by unauthorised users. Hot standby redundancy to be ensured in each control centre. This firewall shall comprise a screening router. The screening router shall filter packets to restrict access based on both source and destination IP addresses. The firewall shall provide the following types of protection:

1. Authentication.
   In order to control unauthorised access to control centre equipment, the firewall shall require authentication of the user.
2. Access Control.
   Based on the identity of the user, different levels of access shall be provided, including none, read only, read/write, and execute.
3. IP Spoofing.

The firewall shall guard against IP spoofing - an attack in which a would-be intruder outside the firewall configures its machine with IP addresses on the internal SCADA LAN.

4. Prevention of Denial of Service (DoS).
   The firewall shall protect against denial of service attacks. These attacks are characterised by attempts to deny service through overrunning buffers, filling the firewall disk, or overrunning the log files. Such attacks shall result in rejection of packets where they can be recognised. Where such packets are not recognised, the firewall shall respond by shutting down or denying external access when overruns occur rather than continuing to operate with partial capability.
5. Packet Filtering and Stateful Inspection.
   The firewall shall provide packet filtering to restrict access based on both source and destination IP addresses. In addition, each packet shall be inspected to determine which port numbers are used by which connections. When a connection closes, access to the port by that connection shall be shut down until another authorised user establishes a new connection.
6. Network Address Translation.
   The firewall shall perform Network Address Translation (NAT) to permit the Employer to hide the IP addresses used on the internal SCADA LAN from external view.
7. Logging.
   The firewall shall provide a comprehensive logging capability to log break-in attempts.
8. Notification.
   The firewall shall provide notification when a break-in attempt is detected.
9. Remote Management.
   A capability shall be provided to permit the Engineer to remotely configure the firewall. Specifically, it shall be possible to remotely disable the firewall's external interface in response to notification of a break-in attempt. The Contractor shall be responsible for the configuration of the firewall, with the Employer's assistance to define the access rules.
10. Cascaded firewalls shall be from different OEM suppliers to ensure a common vulnerability is not easily exploited. Details of the Firewalls in the SCADA LAN will be provided during design stage.

7.2.1 Throughput

Throughput is a vital factor in determining the effectiveness of a firewall in a network. Considering the expected traffic load and future growth, firewall is expected to handle peak traffic without performance degradation. Typically, throughput of the firewall to be in the range of 10-50 Gbps.

7.2.2 Encryption

Firewall Encryption is important to secure the crucial data that passes through it. 256-bit encryption to be in place in order to provide the highest level of security for the sensitive data.

7.2.3 Ports

It shall have minimum 8 Ethernet 10/100/1000 ports (4 ports for connectivity to WAN & 4 Ports for connectivity to LAN) along with 2 SFP ports. Dedicated Management port to be present, allowing administrators to configure the firewall without impacting data traffic. Firmware upgrades, logging or backup procedure to be supported via USB port. Firewall to have a Redundant Power supply port in place for connecting an external power supply to ensure uninterrupted operations.

7.2.4 Port Address Translation

Firewall deployed shall use PAT to aid efficient IP address usage, enhance security and allow for effective traffic management.

7.2.5 DNS Guard

Firewall shall protect the network from various DNS-related threats, reducing the risk of data breaches and malware infections. It shall provide insights into DNS traffic, helping administrators understand how domain names are being resolved and identify anomalies. It shall also prevent users from inadvertently accessing harmful websites, thereby improving the overall endpoint security.

7.2.6 JAVA and ActiveX blocking

Firewall shall perform traffic inspection, Policy-Based Controls, Content filtering and user notifications to help the user, when their attempt to access Java-based content are blocked, in understanding security policies. It shall also perform Protocol Inspection, Policy enforcement, User access control and web filtering for vulnerability mitigation and improve security posture.

7.2.8 Web based management interface

Firewall shall be managed through a web browser with user-friendly dashboard, Configuration management, Real-time monitoring, reporting and logging, multi-user support with different permission levels, Remote access without the need for dedicated client software, customizable views.

7.3 Network Management System

7.3.1 General Requirements

The Contractor shall provide a comprehensive Network Management System (NMS), at each Control Centre that will be used by Employer personnel for network-wide diagnostic monitoring, maintenance, and configuration of the remote communications equipment.

The NMS software shall be compatible with any personal computer running Microsoft Windows 10 (or the latest version of Windows). The Contractor shall provide, install, and configure the software and create the necessary databases for the NMS PC consoles and remote access users. Database provided by contractor to store communication equipment logs should be User friendly and language used should be English. It should be easily accessible to generate reports.

The NMS PC consoles to be provided at both control centres and shall use the latest technology hardware available at the time the Contractor orders them.

BESCOM is upgrading the present INMS system under Up-gradation of DAS System Project. Contractor is responsible for necessary integration to the new INMS system when installed and commissioned.

7.3.2 System Timing and Synchronisation

System-wide timing shall be synchronised to BESCOM DAS NTP server located at the Control Centres. All system equipment requiring a "Clock" signal shall be connected to the System Master Clock source using external clocking.

7.3.3 System Maintainability

Once a failure or degradation of performance is detected in the Communication System, its cause shall be promptly isolated and corrected. To facilitate performance trending, efficient diagnosis, and corrective resolution, the system shall permit in-service diagnostic testing to be executed both locally and from remote locations. Such testing shall not affect the functional operation of the system.

7.3.4 System Expandability

Contractor-supplied equipment and subsystems shall have provisions for expansion accomplished by the addition of plug-in modules and cross-connects. Equipment supplied shall be sized (though not necessarily equipped) to support system/subsystem expansion to full capacity as provided by specified aggregate transmission rates. Equipment units provisioned for unequipped sub-unit expansions shall be terminated at appropriate patching facilities or termination blocks. Power supplies and remote monitoring shall be sized for maximum equipped system capacity.

7.3.5 NMS Functionality

The NMS shall permit network administrators to manage the Remote end equipment from the perspective, for example, of monitoring equipment and link status, responding to reported alarm conditions, performing maintenance forecasting and scheduling activities, configuring the communications equipment, allocating system resources, and administering circuit records.

The NMS central processors shall be co-located with the Communication equipment installed at BCC1 and BCC2. The NMS shall collect real-time data from the communication network equipment and facilities. Data shall be synchronised between BCC1 and BCC2 NMS.

7.3.6 NMS Master Station

The NMS master station function shall provide centralised processing of all NMS data acquisition and control activities. The master station is the high order data processing level of the NMS.

7.3.7 Local Maintenance Interfacing

In addition to NMS master station access, provision shall be made for maintenance personnel to have access to equipment alarms, status, commands, and quality parameters via a local interface port.

7.3.8 User Interface

The USER interface concerns the functionality provided with each NMS workstation. USER interfaces shall be both convenient and responsive. They shall provide the flexibility to adapt to future growth and changes. The minimum user interface requirements are shown in Table 2 below.

Table 2: Minimum User Interface Requirements

Item	Requirement
1	Monitoring via LCD monitor displays and messages
2	Alarm annunciation
3	NMS network configuration control
4	Configuration record maintenance
5	Historical data retrieval
6	Management report generation
7	Event scheduling
8	System resource management

7.3.9 Man-Machine Interactive Requirements

The man-machine interactive requirements address the need for NMS operations to be USER friendly. This shall include easily understood feedback to all USER inputs. System responses shall be quick, clear, complete, and in plain English. Displays shall use colour, blinking, character inversion, and appended symbols to highlight information. Symbols shall also be appended to printed information to highlight alarm data and special messages.

Extensive checks and validations shall be performed on USER entries to detect errors, possible conflicts, and for access authority verification along with login and logout information. Invalid entries and illegal input attempts or actions shall be reported to the USER.

7.3.10 Programmed Displays

All displays shall include the following features:

1. Display heading
2. System line
3. Interactive message area for operator prompts and inputs
4. Date/time
5. Display page number.

The display generator shall be capable of producing graphic depictions for selected display formats. USER edit and creation of displays and display formats shall be provided. The following clause describes the basic displays to be provided by the Contractor.

7.3.11 Tabular Displays

Tabular displays shall list all input and output data, calculated values, and manually entered data for monitoring, remote control, remote test, alarm inhibit, control inhibit, network configuration, and historical functions. As many display pages as are necessary to display all equipped points in the system is required.

Tabular displays shall display points arranged in physical groupings and logical (virtual) groupings. They shall include descriptive text about each point and shall allow the USER to display and change parameters.

7.3.12 Device Overview Displays

These graphical displays shall show the current status of all equipment in the network. Starting at a macro display, the USER shall be able to select and zoom in on more detailed area-selective displays. The final display levels shall provide detailed information about a selected device at the selected location.

7.3.13 Alarm Summary Displays

These displays shall focus on existing alarm conditions and shall include all alarm annunciation details. They shall include a field for remarks on the status of the recovery actions

7.3.14 Event Displays

These displays shall provide a reverse chronological list of all events.

7.3.15 Diagnostic Displays

These displays shall report status and result information for diagnostic tests of remote equipment.

7.3.16 Hardware Event Handling

The NMS shall recognise, report, and log each hardware event including each discreet status point change of state, each command, and command result. In this respect, the NMS shall recognise each discreet sensor point change of state of duration greater than 50 milliseconds as an event,

7.3.17 Alarm Processing

Alarm processing is primarily the function of the NMS. At a minimum, an event defined as an alarm shall be logged with special identifiers and shall be annunciated to direct the attention of the USER to the alarm. An alarm is defined as an event reportable to all event logging devices as well as the NMS.

The NMS shall process alarm events using USER defined masking. This means that the hierarchy of an event shall be consulted by an Alarm Processor to filter or mask other alarms that have resulted because of the primary alarm event. Thus, under a USER defined mask, a transmission link alarm would be reported only with any other associated and specific alarms of interest.

In general, the local response to an alarm condition shall be USER-defined. The localised response may be automatic, may require operator input, or a manual function to be executed.

A controlled response shall be USER-defined to automatically or manually initiate a predetermined sequence of commands/events. This feature shall be structured to support a very flexible combination of commands and events and shall include error checking.

Alarm inhibiting shall cause all alarm processing for the inhibited point to be suspended. An alarm inhibit placed on an existing alarm shall be removed automatically when the alarm condition is rectified. Thus, an alarm inhibit shall not be accidentally left in place to inhibit a future alarm. USER-defined alarm inhibits shall be provided that shall permit programmable alarm inhibit activities.

When an alarm condition is cleared, an annunciation is required that shall direct the USER's attention to the display and/or event log.

7.3.18 Security

Access to database maintenance, command control, and test functions shall be restricted by a security mechanism. Read and write password protection is required. Human error and conflict detection are also required. Repetitive access authority violations shall be an alarm condition reportable as an intrusion.

7.3.19 Security Alarms

A mechanism is required that detects and reports intrusions, such as those detected as physical intrusion events or protected-function violation events, as security alarms,

7.3.20 Human Error and Conflicts

Protected function access violations shall be reported to the offending USER as error messages and warnings. Repetitive violations shall be counted and compared to an adjustable software threshold to determine when access violations are reportable to the security mechanism as an alarm condition.

7.3.21 Historical Retrieval and Storage

The NMS shall store and maintain event records for retrieval as required. Maintenance of the historical records shall include report generation capabilities. Upon request, the INMS shall format and deliver a report based upon a specific historical event or the activities of a device, subsystem, or system within a specified time frame. Minimum one year log records to be maintained in the NMS server.

7.3.22 Report Generator

The NMS shall provide a Report Generation application that produces and delivers reports. The report generator shall permit USER scheduling, additions, deletions and modifications of the structure, content, and delivery of reports.

7.3.23 Help Screens

The NMS shall provide USER-accessible HELP screens. The USER shall access the screens to help execute the applications. HELP screens shall be available to the USER from within the active application and shall not interfere with the activities of the application.

7.4 Cyber Security:

System to be established as per IEC 62443 standard – cyber security for Operational Technology.

The Contractor shall work closely with the Employer to ensure no system security is compromised by the design of the system.

The System shall adhere to existing cyber security policies as per the guidelines of Ministry of Power, GOI and its amendments.

The System software shall be audited immediately before commissioning on-site by a CERT-In Empanelled Cyber Security Auditor to ensure cyber security and IT/OT/IoT Security and Cyber Security Policy of BESCOM are satisfied.

7.4.1 Patch Management

All security patches and upgrades to the operating system and application software shall be tested and certified by the Contractor. All patch management shall be performed by the Contractor at no cost to BESOM until the end of AMC period.

8. Training

The Contractor shall prepare and deliver a comprehensive training program on the operation and maintenance of the Complete Communication System.

The training program shall teach Employer staff the skills needed for database, display, and report construction including verification and maintenance. Software training shall equip Employer staff with the skills required for System maintenance and expansion and for the preparation and integration of new functions. Hardware training shall qualify Employer staff to perform routine preventive maintenance and perform diagnostic tests on the processors, network equipment, and other peripheral equipment.

Table: Course Attendants

Course Name	Attendees per cycle	Location	No of cycle	Estimated Working Days
Communications Overview	10	Employer Site	2	1
Communications Equipment Courses	10	Employer Site	2	1
NMS	10	Employer Site	2	2

9.Testing and Inspection

9.1 Factory Inspections and Tests

Factory inspections and tests shall be performed for the system to ensure compliance with the Technical Specifications. Responsibility for conducting the factory tests shall rest with the Contractor. The Employer (QS&S officials and DAS officials of BESCOM) will perform the communications equipment inspections and witness the factory testing.

The Contractor shall cover Employer representative air travel, ground transportation, and accommodation (including meals) during the required inspection and test witnessing trips. For bidding purposes, up to three representatives shall be taken into account. The Contractor shall take all necessary steps to address and resolve any concerns that the Employer representatives may raise as a result of these activities in a timely fashion. This may result in further inspections and tests until the representatives are fully satisfied that the inspections and tests have been completed successfully. The costs of such additional inspections and tests shall be borne by the Contractor.

The communications equipment shall pass the manufacturer's standard routine tests in accordance with the referenced standards. Certified copies of all routine test results shall be provided as part of the FAT documentation.

No communications equipment shall be shipped until the Employer is satisfied that the approved Factory Acceptance Test (FAT), as based on the inspections, type tests, routine tests, and performance tests below, has been completed successfully. In particular, all variances resulting from FAT shall have been resolved to the Employer's satisfaction prior to shipment.

9.2 Shipment

The communications equipment shall be sufficiently sturdy to withstand handling during shipment, installation, and start-up without damage. The configuration for shipment shall adequately protect the equipment from scraping, banging, or any other damage. The Contractor shall assume responsibility for correction of all such damage prior to final acceptance.

9.3 Link Establishment / Commissioning Tests

As soon as the installation has been completed and put in a tight and clean condition as specified in the Technical Specifications and establishment of link from Control Centre CS equipment, the Contractor shall so notify BESCOM in writing. All sites to be tested from NMS for proper functioning. This will constitute link establishment / commissioning of the links. After verification of the links as per the approved procedure Link establishment certificate to be issued by BESCOM.

Any equipment offline because of power supply issue at SPB end, for link establishment temporary portable batteries to be used by the contractor.

9.4 Availability Test

The Communications System shall be subjected to a One Hundred (100) hours system availability test after link establishment from NMS before being put into commercial service. The purpose of this test is to validate the required in-service availability of the system and its component parts has been met.

Any equipment offline because of power supply issue at SPB end to be excluded from the test.

9.5 Integrated System Test

Sites to be tested for verification of transmission of data from RTUs to control centre. Sample one DI/DO and one AI/AO to be verified. Any issue in the SPB and RTU will not cause failure of the communication test.

10. Warranty and AMC

10.1 Warranty details

The Contractor shall provide Communications System warranty services for a period of two (2) years following Link establishment certificate. All systems and subsystems comprising the Communications System shall be maintained in operational order by the Contractor during this period as per the SLA. Contractor to keep enough spare material to maintain the system healthiness.

10.2 Annual Maintenance Contract

The Contractor shall provide Communications System warranty services for a period of three (3) years following completion of warranty period. All systems and subsystems comprising the Communications System shall be maintained in operational order by the Contractor during this period.

Minor repairs to be rectified by the contractor. Incase of major failure like equipment faulty / Non-repairable equipment will be to BESCOM account. Contractor to facilitate the service upon receipt of new equipment.

10.3 Service Level Agreement

Sl No	Fault Correction	Response time	Contact Method	Restoration time	On site
1	Critical Control Centre Networking equipment	Same day	e-mail	Coordination starts once notified till restoration is achieved.	Within 8 hours on Working Days *
2	Non-Critical Control Centre Networking equipment	Same day on Working Day	e-mail	Coordination starts once notified till restoration is achieved.	If needed, as mutually agreed

3	NMS issue	Same day	e-mail	According to mutually agreed schedule	Within 8 hours on Working Days *
4	Remote Site equipment Issue	Two days	e-mail	According to mutually agreed schedule	If needed, as mutually agreed
5	SIM related issues	Two days	e-mail	According to mutually agreed schedule	If needed, as mutually agreed
6	Leased Line Link issues	Same day	e-mail	Coordination starts once notified till restoration is achieved.	Within 8 hours on Working Days *
7	Any other issue	Same day	e-mail	According to mutually agreed schedule	If needed, as mutually agreed

* Monday to Saturday

10.4 SPARES:

Contractor to maintain spares required for the smooth functioning of the system. BESCOM may be required to provide any or all of the materials to be kept as spares, notifications, and information pertaining to spare parts manufactured or distributed by the Contractor:

(a) such spare parts as BESCOM may elect to purchase from the Contractor, providing that this election shall not relieve the Contractor of any warranty obligations under the Contract; and

(b) In the event of termination of production of the spare parts:
   (i) advance notification to BESCOM of the pending termination, in sufficient time to permit the BESCOM to procure needed requirements; and
   (ii) following such termination, furnishing at no cost to BESCOM, the blueprints, drawings and specifications of the spare parts, if requested.

The Contractor shall carry sufficient inventories to assure ex-stock supply of spares required for the project. List of Spare material to be given in the format as per Annexure G: Bid Form. Other spare parts and components shall be supplied as promptly as possible but in any case within 1 month of placement of order.